AMENDMENTS TO THE CLAIMS

Upon entry of the present amendment, the status of the claims will be as is shown below. This listing of claims replaces all previous versions and listings of claims in the present application.

Listing of Claims:

1. (Currently Amended) A data encryption method, the method comprising:

constructing a security class database for storing a plurality of entries of records of data, each of the plurality of entries of records including a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators, wherein at least one of the plurality of encryption algorithm module indicators indicates an asymmetric encryption algorithm and at least one of the plurality of encryption algorithm module indicators indicates a symmetric encryption algorithm;

inputting digital data to be encrypted;

from the security class database, finding each data attribute description that matches an attribute of the digital data, and retrieving the corresponding encryption definition data;

from the retrieved encryption definition data, selecting at random an encryption value related to [[an]] one of the plurality of encryption algorithm module ~~indicator~~ indicators;

with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data, wherein the encryption algorithm

module indicator dynamically maintains a balance between security level and processing speed; and

appending decryption information to the digital data that has undergone encryption processing for subsequent output.

2. (Previously Presented) The method as claimed in Claim 1, wherein the encryption definition field in the constructed security class database includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby, an encryption algorithm module indicator being selected from the retrieved encryption definition data according to each of the encryption algorithm module indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

3. (Previously Presented) The method as claimed in Claim 1, wherein the encryption definition field in the constructed security class database includes a plurality of encryption algorithm module combinations, each of the encryption algorithm module combinations containing an encryption algorithm module indicator and an authentication algorithm module indicator, an encryption algorithm module combination being retrieved at random from the retrieved encryption definition data, the selected encryption algorithm module combination being used as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

4. (Previously Presented) The method as claimed in Claim 3, wherein the encryption definition field in the constructed security class database includes a plurality of encryption algorithm module combinations and corresponding proportions adopted thereby, an encryption algorithm module combination being selected from the retrieved encryption definition data according to each of the encryption algorithm module combinations and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

5. (Currently Amended) A data encryption method, the method comprising:

constructing an encryption module database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing an encryption algorithm module indicator and an authentication algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm;

constructing a security class database for storing a plurality of entries of records of data, each of the plurality of entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption module database indexes;

inputting digital data to be encrypted;

from the security class database, finding each data attribute description that matches an attribute of the digital data, and retrieving the corresponding encryption definition [[data]] field;

from the retrieved encryption definition [[data]] field, selecting at random [[an]] one of the plurality of encryption module database [[index]] indexes;

according to the retrieved encryption module database index, selecting an entry of record from the encryption module database;

with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data, wherein the selected entry of record dynamically maintains a balance between security level and processing speed; and

appending decryption information to the digital data that has undergone encryption processing for subsequent output.

6. (Previously Presented) The method as claimed in Claim 5, wherein the encryption definition field in the constructed security class database includes a plurality of encryption module database indexes and corresponding proportions adopted thereby, an encryption module database index being selected from the retrieved encryption definition data according to each of the encryption module database indexes and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

7. (Currently Amended) A data encryption method, the method comprising:

constructing encryption definition data containing a plurality of encryption algorithm module indicators, wherein at least one of the plurality of encryption algorithm module indicators indicates an asymmetric encryption algorithm and at least one of the plurality of encryption algorithm module indicators indicates a symmetric encryption algorithm;

inputting digital data to be encrypted;

from the encryption definition data, selecting at random [[an]] one of the plurality of encryption algorithm module ~~indicator~~ indicators;

with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data, wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed; and

appending decryption information to the digital data that has undergone encryption processing for subsequent output.

8. (Previously Presented) The method as claimed in Claim 7, wherein the constructed encryption definition data includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby, an encryption algorithm module indicator being selected from the encryption definition data according to each of the encryption algorithm module indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

9. (Previously Presented) The method as claimed in Claim 7, wherein the constructed encryption definition data includes a plurality of encryption algorithm module combinations, each of the encryption algorithm module combinations including an encryption algorithm module indicator and an authentication algorithm module indicator, an encryption algorithm module combination being selected at random from the retrieved encryption definition data, the selected encryption algorithm module combination being used as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

10. (Previously Presented) The method as claimed in Claim 9, wherein the constructed encryption definition data includes a plurality of encryption algorithm module combinations and corresponding proportions adopted thereby, an encryption algorithm module combination being selected from the retrieved encryption definition data according to each of the encryption algorithm module combinations and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

11. (Currently Amended) A data encryption method, the method comprising:

constructing an encryption module database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing an encryption algorithm module indicator and an authentication algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of

data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm;

constructing encryption definition data which includes a plurality of encryption module database indexes;

inputting digital data to be encrypted;

from the encryption definition data, selecting at random an encryption module database index;

according to the retrieved encryption module database index, selecting an entry of record from the encryption module database;

with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data, wherein the selected entry of record dynamically maintains a balance between security level and processing speed; and

appending decryption information to the digital data that has undergone encryption for subsequent output.

12. (Previously Presented) The method as claimed in Claim 11, wherein the encryption definition data includes a plurality of encryption module database indexes and corresponding proportions adopted thereby, an encryption module database index being selected from the encryption definition data according to each of the encryption module database indexes and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

13. (Currently Amended) A data encryption method, the method comprising:

constructing a security class database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing a data attribute description field and a corresponding encryption definition field, the encryption definition data field being an encryption algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm;

inputting digital data to be encrypted;

from the security class database, finding each data attribute description field that matches an attribute of the digital data, and retrieving the encryption algorithm module indicator of the corresponding encryption definition data field;

with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data, wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed; and

appending decryption information to the digital data that has undergone encryption processing for subsequent output.

14. (Previously Presented) The method as claimed in Claim 13, wherein the constructed encryption definition field in the security class database is an encryption algorithm module combination, the encryption algorithm module combination including an encryption algorithm module indicator and an authentication algorithm module indicator, data of an encryption algorithm module combination of the corresponding encryption definition field being retrieved in finding from the security class database the data attribute description that matches the attribute of the digital data, the selected encryption algorithm module combination being used as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

15. (Currently Amended) A data encryption method, the method comprising:

constructing an encryption module database for storing a first plurality of entries of records of data, each of the plurality of entries of records of data containing an encryption algorithm module indicator and an authentication algorithm module indicator, wherein the encryption algorithm module indicator of one of the first plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the first plurality of entries of records of data indicates a symmetric encryption algorithm;

constructing a security class database for storing a second plurality of entries of records of data, each of the second plurality of entries of records of data containing a data

attribute description field and a corresponding encryption definition field, the encryption definition data field being an encryption module database index;

inputting digital data to be encrypted;

from the security class database, finding each data attribute description field that matches an attribute of the digital data, and retrieving the encryption module database index from the corresponding encryption definition field;

with the retrieved encryption module database index as a guide, selecting an entry of record from the encryption module database;

with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data, wherein the selected entry of record dynamically maintains a balance between security level and processing speed; and

appending decryption information to the digital data that has undergone encryption processing for subsequent output.

16. (Currently Amended) A data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising:

a security class database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators, wherein at least one of the plurality of encryption algorithm module indicators indicates an asymmetric encryption algorithm

and at least one of the plurality of encryption algorithm module indicators indicates a symmetric encryption algorithm;

an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data;

a parameter processing portion for updating the security class database with the parameter data sent from the inspecting portion;

an attribute inspecting portion for finding from the security class database each data attribute description that matches an attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to an encryption selecting portion;

the encryption selecting portion, selecting at random, an encryption algorithm module indicator from the retrieved encryption definition data; and

an encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected by the encryption selecting portion as a guide, wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed.

17. (Original) The apparatus as claimed in Claim 16, wherein the encryption definition field in the security class database includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby, the encryption selecting portion selecting an encryption algorithm module indicator from the retrieved encryption definition data according to each of the encryption algorithm module

indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

18. (Original) The apparatus as claimed in Claim 16, wherein the encryption definition field in the security class database includes a plurality of encryption algorithm module combinations, each of the encryption algorithm module combinations including an encryption algorithm module indicator and an authentication algorithm module indicator, the encryption selecting portion selecting at random an encryption algorithm module combination from the retrieved encryption definition data, the encryption processing portion, using the encryption algorithm module combination selected by the encryption selecting portion as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

19. (Original) The apparatus as claimed in Claim 18, wherein the encryption definition field in the security class database includes a plurality of encryption algorithm module combinations and corresponding proportions adopted thereby, the encryption selecting portion selecting an encryption algorithm module combination from the retrieved encryption definition data according to each of the encryption algorithm module combinations and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

20. (Previously Presented) The apparatus as claimed in Claim 16, further comprising:

an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator;

the encryption definition field of the security class database including a plurality of encryption module database indexes;

the encryption selecting portion selecting at random an encryption module database index from the retrieved encryption definition data and, according to the retrieved encryption module database index, and selecting an entry of record from the encryption module database;

the encryption processing portion using the entry of record selected by the encryption selecting portion as a guide to control encryption processing, including the type of encryption and the type of authentication, of the inputted digital data, wherein the selected entry of record dynamically maintains a balance between security level and processing speed.

21. (Original) The apparatus as claimed in Claim 20, wherein the encryption definition field in the security class database includes a plurality of encryption module database indexes and corresponding proportions adopted thereby, the encryption selecting portion selecting an encryption module database index from the retrieved encryption definition data according to each of the encryption module database indexes and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation, and selecting an entry of record from the encryption module database according to the retrieved encryption module database index.

22. (Original) The apparatus as claimed in Claim 20, wherein the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion.

23. (Currently Amended) A data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising:

a encryption module database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing an encryption algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm;

an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data;

a parameter processing portion for updating the encryption module database using the parameter data from the inspecting portion;

a encryption selecting portion for selecting at random an entry of record from the encryption module database; and

an encryption processing portion for controlling encryption processing of the inputted digital data using the entry of record selected by the encryption selecting portion

as a guide, wherein the selected entry of record dynamically maintains a balance between security level and processing speed.

24. (Original) The apparatus as claimed in Claim 23, wherein the encryption module database stores a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and a corresponding proportion adopted thereby, the encryption selecting portion selecting an entry of record according to the corresponding proportion adopted by each of the entries of records in the encryption module database in cooperation with a random number generator and a MOD operation.

25. (Original) The apparatus as claimed in Claim 23, wherein the encryption module database stores a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator, the encryption processing portion controlling encryption processing, including the type of encryption and the type of authentication, using an encryption algorithm module combination of the entry of record selected at random by the encryption selecting portion as a guide.

26. (Original) The apparatus as claimed in Claim 25, wherein the encryption module database stores a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator, an authentication algorithm module indicator and corresponding proportions adopted thereby, the encryption

selecting portion selecting an entry of record from the encryption module database according to the corresponding proportion adopted by each entry of record in the encryption module database in cooperation with a random number generator and a MOD operation.

27. (Currently Amended) A data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising:

a security class database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing a data attribute description field and a corresponding encryption definition field, the encryption definition field being an encryption algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm;

an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data;

a parameter processing portion for updating the security class database with the parameter data from the inspecting portion;

an attribute inspecting portion for finding from the security class database each data attribute description that matches an attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to an encryption processing portion; and

the encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected by the attribute inspecting portion as a guide, wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed.

28. (Original) The apparatus as claimed in Claim 27, wherein the encryption definition field in the security class database is an encryption algorithm module combination, the encryption algorithm module combination including an encryption algorithm module indicator and an authentication algorithm module indicator, the encryption processing portion, using the encryption algorithm module combination selected by the parameter inspecting portion as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data.

29. (Currently Amended) A data decryption method, the method comprising:

inputting digital data to be decrypted;

inspecting to determine whether the digital data includes a decryption algorithm module indicator and, upon an affirmative determination, retrieving the decryption algorithm module indicator from a decryption module database which stores a plurality of decryption algorithm module indicators, with at least one of the plurality of decryption algorithm module indicators indicating an asymmetric decryption algorithm and at least one of the plurality of decryption algorithm module indicators indicating a symmetric

decryption algorithm and, upon a negative determination, setting the data to be decrypted as equivalent to inputted data for subsequent processing;

with the retrieved decryption algorithm module indicator as a guide, controlling decryption processing of the inputted digital data, wherein the retrieved decryption algorithm module indicator dynamically maintains a balance between security level and processing speed; and

outputting the digital data that has undergone decryption.

30. (Previously Presented) The method as claimed in Claim 29, wherein the digital data is inspected to determine whether the digital data includes a decryption algorithm module combination having a decryption algorithm module indicator and an authentication algorithm module indicator and, upon an affirmative determination, the decryption algorithm module combination is retrieved or, upon a negative determination, the data to be decrypted is set to be equivalent to inputted data for subsequent processing; and controlling decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the selected decryption algorithm module combination as a guide.

31. (Currently Amended) A data decryption method, the method comprising:

constructing a decryption module database for storing a plurality of entries of records of data, each of the plurality of entries of records of data being a decryption algorithm module indicator, wherein one of the plurality of entries of records of data

being a decryption algorithm module indicator indicates an asymmetric decryption algorithm and another of the plurality of entries of records of data being a decryption algorithm module indicators indicates a symmetric decryption algorithm;

inputting digital data to be decrypted;

inspecting to determine whether the digital data includes a decryption module database index and, upon an affirmative determination, retrieving the decryption module database index or, upon a negative determination, setting the data to be decrypted as equivalent to inputted data for subsequent processing;

with the retrieved decryption module database index as a guide, selecting an entry of record from the decryption module database;

with the selected entry of record as a guide, controlling decryption processing of the inputted digital data, wherein the selected entry of record dynamically maintains a balance between security level and processing speed; and

outputting the digital data that has undergone decryption.

32. (Previously Presented) The method as claimed in Claim 31 a decryption module database for storing a plurality of entries of records of data is constructed, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, and the selected entry of record is used as a guide for controlling decryption processing, including the type of decryption and the type of authentication, of the inputted digital data.

33. (Currently Amended) A data decryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after decryption processing thereof, the apparatus further comprising:

an inspecting portion for inspecting whether the data inputted via the input portion includes a decryption algorithm module indicator and, upon an affirmative inspection result, retrieving the decryption algorithm module indicator from a decryption module database which stores a plurality of decryption algorithm module indicators, with at least one of the plurality of decryption algorithm module indicators indicating an asymmetric decryption algorithm and at least one of the plurality of decryption algorithm module indicators indicating a symmetric decryption algorithm or, upon a negative inspection result, transmitting the inputted data directly to the output portion; and

a decryption processing portion for controlling decryption processing of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide, wherein the retrieved decryption algorithm module indicator dynamically maintains a balance between security level and processing speed.

34. (Previously Presented) The apparatus as claimed in Claim 33, wherein the inspecting portion inspects whether the data inputted via the input portion includes a decryption algorithm module combination, the decryption algorithm module combination including a decryption algorithm module indicator and an authentication algorithm module indicator, and, upon an affirmative inspection result, retrieves the decryption algorithm module combination or, upon a negative inspection result, directly transmits the inputted data to the output portion, the decryption processing portion controlling the

decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide.

35. (Previously Presented) The apparatus as claimed in Claim 33, further comprising: a decryption module database for storing a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator, the inspecting portion inspecting whether the data inputted via the input portion includes a decryption module database index and, upon an affirmative inspection result, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index and upon a negative inspection result, directly transmitting the inputted data to the output portion, the decryption processing portion controlling the decryption processing of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide.

36. (Original) The apparatus as claimed in Claim 35, wherein the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion controlling decryption processing, including the type of decryption and the type of authentication, using the entry of record retrieved by the inspecting portion as a guide.

37. (Previously Presented) The apparatus as claimed in Claim 35, further comprising: a parameter processing portion for updating the decryption module database using parameter data, the inspecting portion inspecting and separating the data inputted via the input portion into parameter data or digital data and, if the inputted data is parameter data, transmitting the same to the parameter processing portion and, if the inputted data is digital data, inspecting whether the digital data includes a decryption module database index and, upon an affirmative inspection result, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index and, upon a negative inspection result, directly transmitting the inputted data to the output portion.

38. (Original) The apparatus as claimed in Claim 37, wherein the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion controlling decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide.

39. (Original) The apparatus as claimed in Claim 21, wherein the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion.